1

Table of Contents

6.0 Security Standards

6.0.1 Security Overview

Section 6.0 addresses four new, specific aspects of voting systems security. These new items are:

1. Definitions for Independent Verification Voting Systems: definition of voting systems that produce multiple records of votes. A future version of the VVSG will require that voting systems produce multiple records of ballots or receipts for auditing purposes.

2. Security Requirements for Voter Verified Paper Audit Trails: requirements for voter verified paper audit trails, if a State chooses to require them.

3. Use of Wireless Networking in Voting Systems: how wireless networks and the data sent across wireless networks should be secured.

4. Security Requirements for Software Distribution and Setup Validation of Voting System: requirements for the secure distribution of voting systems software and ballot information for verifying that voting systems are operating with the correct software and software configuration.

The remainder of Section 6.0 is an informative section with discussion of independent verification systems followed by definitions of the types of independent verification systems which will be used as the basis for future requirements. The definitions are preliminary and will be evolving with further research.

6.0.1.1 Independent Verification Systems (Informative)

The primary objective for using electronic voting systems is the production of voting records that are highly precise, highly reliable, and easily counted - in essence, an accurate representation of ballot choices whose handling requirements are reasonable. To meet these objectives, there are many factors to consider in an electronic voting system's design, including:

- the environment provided for voting, including the voting site and various environmental factors,
- the ease with which voters can use the voting system, i.e., its usability,
- the robustness and reliability of the voting equipment, and
- the capability of the records to be used in audits.

Independent Verification systems have as their primary objective the production of ballot records that are capable of being used in audits in which their correctness can be audited to very high levels of precision. The primary security issues addressed by independent verification systems are:

- whether electronic voting systems are accurately recording ballot choices, and
- whether the ballot record contents can be audited precisely post-election.

The threats addressed by independent verification systems are those that could cause a voting system to inaccurately record the voter's intent or cause a voting system's records to become damaged, i.e., inserted, deleted, or changed. These threats could occur via any number of means including accidental damage or various forms of fraud. The threats are addressed mainly by providing, in the voting system design, the capability for ballot record audits to detect precisely whether specific records are correct as recorded or damaged, missing, or fraudulent.

6.0.1.1.1 Problems in Auditing Single Record Voting Systems

The auditing paradigm in financial transactions, e.g., transactions in which a merchant retains a copy of the transaction and the purchaser retains a receipt that can be reviewed for accuracy, does not apply for voting systems. This poses a complication for election officials and voters when seeking the same high degrees of assurance that ballots cast on electronic voting systems are being recorded and counted correctly.

Electronic voting systems that produce a sole record of cast ballots are inherently limited in their capability for accurate audits - as would a financial system that produced only one record of its transactions[1]. When there is only one record, the assurance that the cast ballots are being correctly recorded by the voting system is limited to other means such as:

- confidence in how well the voting system was inspected and tested,
- logic and accuracy tests performed pre-election,
- parallel testing of voting equipment on election day,
- inspection of the voting system's event log for anomalous behavior,
- comparison of election results with post-election polls, and
- comparison of election results with expected voter behavior.

It is highly desirable that electronic voting systems be designed such that they already include, as a fundamental part of their design, the mechanisms to provide highly accurate and reliable auditing of ballot contents.

6.0.1.1.2 Independent Verification Systems: Improved Accuracy in Audits

Independent Verification is the top-level categorization for electronic voting systems that produce multiple records of ballot choices whose contents are capable of being audited to high levels of precision. For this to happen, the records must be produced, verified by the voter, and subsequently handled according to the following protocol:

[1] Electronic voting systems that create and store copies of their electronic records or that print a copy of their electronic records in effect store just one record of cast ballots because the additional records are clones of the first record. The additional records cannot be used to audit the accuracy of the first record.

(a) At least two records of the voter's choices are produced and one of the records is then stored such that it cannot be modified by the voting system, e.g. the voting system creates a record of the voter's choices and then copies it to some write-once media.

(b) The voter must verify that both records are correct, e.g., verify his or her choices on the voting system's display and also verify the second record of choices stored on the write-once media.

(c) The verification processes for the two verifications must be independent of each other and (a) at least one of the records must be verified directly by the voter, or (b) it is acceptable for the voter to indirectly verify both records if they are stored on different systems produced by different vendors.

(d) The content of the two records can be checked later for consistency through the use of identifiers that allow the records to be linked.

An assumption is made that at least one set of the records is usable in an efficient counting process, such as by using an electronic voting system, and the other set of records is usable in an efficient process of verifying its agreement with the first set of records. The other set records would preferentially be different in form from the first set of records and have some resistance to accidental or deliberate damage.

Given these conditions above, the multiple records are said to be *distinct* and *independently verifiable*, that is, both records are not under the control of the same processes. As a result of this independence, one record can be used to audit or check up on the accuracy of the other record. Because the storage of the records is separate, an attacker who can compromise one of these records still will face a difficult task in compromising the other.

A simple example of an independent verification system is an electronic voting station that records a voter's choices and then writes them to a token. If the voter removes the token and inserts it into a separate system that makes an electronic copy of the token and displays it to the voter, the voter can then verify that the first station has recorded the ballot correctly and the second station has copied and stored the ballot correctly. This example satisfies the four conditions necessary for handling multiple records in independent verification systems, as follows:

- Condition (a) is satisfied because two records are created and the record stored on the token cannot be modified by the same system used to create the electronic copy.

- Condition (b) is satisfied because the voter verifies at the second station that the record stored on the token is accurate and verifies at the second station that the copy of the token's record made by the second station is correct.

- Condition (c) is satisfied because the voter is able to directly verify that the record stored on the token is accurate -- the verification of the second record is indirect, because the same voting system that created the separate record is being used to verify it.

- Condition (d) satisfied because the records are created so that the record on the token can identify its copy stored by the voting system (this wasn't included in the example but is assumed to happen).

There are many types of independent verification systems. This example is a split process system, as described in Section 6.0.1.1.3.1.

6.0.1.1.3 Example Independent Verification Systems

The following sections contain informative overviews of several types of independent verification systems, some of which have not been implemented yet. Thus their inclusion in this document is intended to help clarify approaches to independent verification systems. The systems discussed are:

- voting systems with a split process architecture,
- end-to-end voting systems that include cryptographic audit schemes,
- witness voting systems that take a picture of or otherwise capture an indirect verification of ballot choices,
- direct independent verification, including some types of voting systems that produce an optically scanned ballot or that produce a voter-verified paper audit trail (VVPAT).

6.0.1.1.3.1 The Split Process Architecture for Independent Verification Systems

A voting machine in this scheme consists of vote capture and verification stations that are kept separate, i.e., two physical devices. A voter inserts an object called a token into the capture station to make ballot selections, and then takes the token object to the verification station to review and store his or her votes. The token

object could be paper or some write-once read-only media. Two records of the vote are created: one on the token object and one by the verification station. Either could be used in the final count.[2]

Any split process voting system, the interaction between the voter and the split process is operates as follows:

1. A voter is given a token object that has been initialized to be blank.

2. Supporting information is written to the token object including the ballot and identification information about the election and precinct.

3. The voter inserts the token object into a capture station such as a DRE, which reads the ballot information from the token and then displays the ballot on an input device such as a touch screen. The voter then makes his or her ballot choices and then causes a record of the vote to be recorded on the token object.

4. The voter then takes the token object to a separate verification station, which reads the recorded votes from the token object, makes an electronic copy, and displays it to the voter.

5. The voter verifies that the information is correct and then deposits the token object into a container where it can be archived and used later for recounts or audits against the electronic records.

The electronic records recorded by the verification station typically would be counted in the election. One of the records should preferentially be different in form from the other record and have some resistance to accidental or deliberate damage so that it can remain useful for audits and recounts.

In theory, the physical separation of the ballot capture from the ballot verification may make analysis of the capture and verification devices easier or less costly. The rationale is that the user interface software on the capture station can be expected to be complex and

[2] The split process architecture is otherwise known as the frog protocol, which was first described in the Caltech – MIT report: voting*: What Is, What Could Be*, as part of a modular voting architecture. The frog term, i.e., the token, was chosen specifically to convey no information about the physical form of the object used to carry vote information between two separate modules of the voting station. The report is available for download at http://www.vote.caltech.edu/.

difficult to verify for correctness. On the other hand, the verification station's software can be expected to be less complicated because it need only copy the contents of the token, display it to the voter, and then store the ballot choices.

The verification station's software can be considered to be the "trusted computing base" of the voting system, because it must be trusted in the verification process and then trusted to store the record for counting, i.e., cast the voter's ballot. Its software should be relatively small and thus easier to inspect and test.

In general, segregating functions by placing them on physically different systems is a standard computer security practice for making those functions easier to test for correctness and easier to manage securely.

6.0.1.1.3.2 End to End (Cryptographic) Independent Verification Systems

End to end voting systems use cryptographic techniques to store an encrypted copy of the voter's ballot choices and to give the voter the option to verify the correct recording and inclusion of his or her vote in the election totals. In this way, ballots can be audited and demonstrated to have been included in the final tally.

End to end systems in existence today generally operate as follows:

1. A voter uses a voting station such as a DRE to make ballot choices.

2. The DRE then issues a paper receipt to the voter that contains information that permits the voter to verify that the choices were recorded correctly. The information does not permit the voter, though, to reveal his or her choices.

3. The voter may have the option to check that his or her ballot choices were included in the final tally, e.g., by checking a web site of values that (should) match the information on the voter's paper receipt.

End to end systems are sometimes referred to as *receipt-based* systems. They may provide an assurance not only that the correct set of ballot choices was recorded, but that those choices were included in the election count. Some analyses of auditing and cryptographic

systems assert that very small numbers of self-audits are required to verify the correctness of an election.

6.0.1.1.3.3 Witness Independent Verification Systems

A witness voting system creates the second record of ballot choices by using a separate module to record or witness the voter's verification of the first record. The primary feature of a witness system that recommends itself is that the creation of the record does not require action by the voter. This may result in quicker voting times or voting systems that are simpler to use than some other schemes that involve multiple, direct verifications by the voter.

An example of a witness system is a DRE with a camera mounted above its screen. The camera takes pictures and saves them independently of the DRE. It would operate as follows:

1. A voter makes ballot choices at the DRE and then presses a button to record his or her vote.

2. The DRE records the ballot choices and uses them in the election count.

3. At the time the button is pressed, the camera takes a picture of the DRE's screen and saves the image (the voter is not included in the picture).

4. This collection of images constitutes a second ballot record that can be used in audits and recounts of the records recorded by the DRE.

As can be seen by this example, the voter's interactions are reduced to making ballot choices at the DRE and pressing a button to make the selections final. If the DRE were to have been compromised such that it secretly recorded the ballot choices incorrectly, the stored photographic images would reflect what the voter had seen and verified at the DRE's screen.

Because the voter cannot verify that the creation of the second record was performed accurately, a requirement of this type of system is that the creation process must be highly reliable and very resistant to accidental or deliberate damage. Also, the suitability of the records for manual or automated auditing must be considered in their selection.

6.0.1.1.3.4 Direct Independent Verification Systems

Direct independent verification systems produce a record for voter verification that the voter may verify directly with the voter's senses and which is then preserved for auditing or possibly counting. Some optical scan voting system schemes fit into this category (albeit loosely), as well as those systems with VVPAT (Voter Verified Paper Audit Trail) capability.

The type of optical scan voting systems schemes in this category are those in which two records are created: a paper and an electronic record. This system uses Optical Scan Recognition (OCR) to create an electronic record from the paper record after the paper record has been directly verified by the voter. The general operation of this system is:

1. A voter uses a marking device such as a DRE to mark a ballot and then presses a button to print the marked ballot onto a piece of paper.

2. The voter then directly reviews the paper to ensure its correctness, and if correct, places the paper record into a scanner (some procedure would need to be included to handle spoiled ballots).

3. The scanner converts the paper record into an electronic format. To reduce errors that may result from scanning the paper record, the paper records might contain a barcoded representation of the human readable portion of the ballot.

4. The paper record gets preserved in a ballot box.

The reason that the above scheme fits loosely into the independent verification category is because only one of the records was verified. One may assume that the scanning process is highly accurate and can be trusted to create the electronic record correctly; however it would be preferential for the voter to somehow verify that the record was, in fact, created correctly.

An electronic voting system with VVPAT (Voter Verified Paper Audit Trail) capability is similar to that of the optical scan above but consists typically of a DRE that both creates and records an electronic record, and printer to create a paper audit trail of the voter's choices. Like the optical scan system, it creates two distinct

representations of the voters' ballot choices: an electronic record and a paper record.

Typically, a voter would use the voting system (called a DRE-VVPAT) as follows:

1. A voter makes ballot selections and then indicates that his or her selections are complete.

2. The VVPAT-DRE prints a paper record summary of the voter's ballot choices. An alternative approach to VVPAT involves printing the voter's ballot selections as they are made, e.g., a concurrent or contemporaneous record.

3. The voter inspects and directly verifies that the paper record matches the displayed electronic record (again, a procedure would need to be included to handle spoiled ballots).

4. The paper record gets preserved in a ballot box.

Both schemes described here produce paper records that are verified directly by sight. Voters with sight impairments require an accessible device for verification that can produce an audible representation of the paper record.

6.0.1.1.4 Issues in Handling Multiple Records Produced by Independent Verification Systems

There are several fundamental questions that need to be addressed when designing the structure and selecting the physical characteristics of independent verification voting systems records, including:

- how to tell if the records are authentic and not forged,
- how to tell if the integrity of the records has remained intact from the time they were recorded,
- the suitability of the records for various types of auditing, and
- how best to address problems if there are errors in the records.

Whenever an electronic voting system produces multiple records of votes, there is some possibility that one or more of the records may not match. Records can be lost, or deliberately or accidentally damaged, or stolen, or

fabricated. Keeping the two records in correspondence with each other can be made more or less difficult depending on the technologies used for the records and the procedures used to handle the records.

As a consequence, it is important to structure the records so that errors and other anomalies can be readily detected during audits. There are a number of techniques that can be used, such as the following:

- associating unique identifiers with corresponding records, e.g., an individual paper record sharing a unique identifier with its corresponding electronic record,

- including an identification of the specific voting system that produced the records, such as a serial number identifier or by having the voting system digitally sign the records using public key cryptography,

- including other information about the election and the precinct or location where the records were created,

- creating checksums of the electronic records and having the voting system digitally sign the entire sets of records so that missing or inserted records can be detected, and

- structuring the records in open, publicly documented formats that can be readily analyzed on different computing platforms

The ease or relative difficulty with which some types of records must be handled is also a determining factor in the practical capability to conduct precise audits, given that some types of records are better suited to different types of auditing and different voting environments than others. The factors that make certain types of records more suitable than others could vary greatly depending upon many other criteria, both objective and subjective. For example, paper records may require manual handling by voters or poll workers and thus be more susceptible to damage or loss. At the same time, the extent to which the paper records must be handled will vary depending on the type of voting system in use. Electronic records may by their nature be more suitable for automated audits; however electronic records are still subject to accidental or deliberate damage, loss, and theft.

It is not possible to discuss all factors and criteria that might make some records more suitable than others. Other procedures used in elections to help maintain the authenticity and integrity of records can also be affected by the suitability of the records, including procedures for comparing the

count of cast ballots with the signatures of voters who cast the ballots, or procedures for maintaining accurate counts of how many ballots or cast on each voting system, or procedures for observing secure chains of custody of ballots. As stated previously, there may be subjective criteria for deciding which type of record is most suitable, e.g., a preference for paper despite its handling issues.

Lastly, the questions of what to do when problems occur and which records thus should be counted in the election can be difficult to answer. It can depend on which record is damaged, whether multiple records are damaged, and what the damage may indicate: ballot fraud, accidental damage, missing ballots, sabotage of the voting system, etc. Depending on how the records are damaged, it may require use of both records to reconstruct the complete record of voters' choices. Obviously, the more supporting evidence that is maintained in the structure of the record, the better equipped one is to make judgments as to which record to use.

6.0.1.2 Core Definitions for Independent Verification Systems (Informative)

This section contains a preliminary set of definitions for independent verification systems. These definitions are fundamental in nature and apply to all categories of independent verification systems. The remaining sections (following this section) contain definitions that are specific to those categories discussed in the preceding sections (split process, end to end, witness, and direct). The definitions will form the basis for future requirements for independent verification systems.

6.0.1.2.1 An independent verification voting system produces two distinct records of ballot choices via interactions with the voter whose equality of content can be audited to verify that the ballot choices were recorded accurately.

Responsible Entity: voting system vendor
Process: voting

Discussion: This is the fundamental core definition for independent verification systems. The records can be checked against one another to determine whether or not the voter's choices were being correctly recorded.

6.0.1.2.1.1 The voter verifies the content of each record and either (a) verifies at least one of the records directly or (b) verifies both records indirectly if the records are each under the control of independent processes.

Responsible Entity: voting system vendor
Process: voting

Discussion: A record can be verified directly by using senses, e.g., by sight, by ear. Indirect verification is when a technically and physically distinct module captures and makes a recording of the voter's verification of a record.

6.0.1.2.1.2 The creation, storage, and handling of the records are sufficiently separate such that the failure or compromise of one record does not cause the failure or compromise of another.

Responsible Entity: voting system vendor
Process: voting

Discussion: The records must be stored on different media and handled independently of each other, so that no one process could compromise all records. If an attack can alter one record, it should still be very difficult to alter the other record.

6.0.1.2.1.2.1 At least one record is highly resistant to damage or alteration and should be capable of long-term storage.

Responsible Entity: voting system vendor
Process: voting

Discussion: At least one of the records should be difficult to alter or damage so that it could be used in case the counted records are damaged or lost.

6.0.1.2.1.3 The processes of verification for the multiple records do not all depend for their integrity on the same device, software module, or system, and are sufficiently separate such that the records each provide evidence of the voter's choices independently of the other records.

Responsible Entity: voting system vendor
Process: voting

Discussion: For example, the verification of an electronic record on a DRE is not sufficiently separate from the verification of an electronic record located on a token but performed on the same DRE as the verification for the first record. Verification of a paper record by one's senses is sufficiently separate, in this case.

6.0.1.2.1.4 The records can be used in audits of one another, so that at least one set of records can be used in an efficient counting process, and another set of records can be used in an efficient process of verifying its substantial agreement with the first set of records.

Responsible Entity: voting system vendor
Process: voting

Discussion: For example, an electronic record can be used in an efficient counting process. A second paper record can be used to verify the accuracy of the electronic record; however its suitability for efficient counting is less clear. If a paper record can be used in an automated scan process, it may be more suitable.

6.0.1.2.1.5 The records include an identification of the voting site/precinct.

Responsible Entity: voting system vendor
Process: voting

Discussion: If the voting site and precinct are different, both should be included.

6.0.1.2.1.6 The records include information identifying whether the balloting is provisional, early, or on Election Day, and information that identifies the ballot style in use.

Responsible Entity: voting system vendor
Process: voting

6.0.1.2.1.7 The records include a voting session identifier that is generated when the voting station is placed in voting mode and that can be used to identify the records as being created during that voting session.

Responsible Entity: voting system vendor
Process: voting

Discussion: If there are several voting sessions on the same voting station on the same day, the voting session identifiers must be different. They should be generated from a random number generator.

6.0.1.2.1.8 The records include an identifier of the voting system that is unique to that style of voting systems.

Responsible Entity: voting System
Process: voting

Discussion: The identifier could be a serial number or other unique ID.

6.0.1.2.1.9 All cryptographic software in independent verification voting systems is in modules that have been approved by the U.S. Government's Crypto Module Validation Program (CMVP) as applicable.

Responsible Entity: voting system vendor
Process: voting

Discussion: The voting systems may use cryptographic software for a number of different purposes, including calculating checksums, encrypting records, authentication, generating random numbers, and for digital signatures. This software should be reviewed and approved by the Crypto Module Validation Program. There may be cryptographic voting schemes where the cryptographic algorithms used are necessarily different from any algorithms that have approved CMVP implementations, thus CMVP approved software should be used where feasible. The CMVP web site is http://csrc.nist.gov/cryptval.

6.0.1.3 Split Process Independent Verification Systems (Informative)

This section contains definitions specific to split process independent verification systems. The definitions build on and are in addition to the core definitions in Section 6.0.1.2. Split process systems consist of separate vote capture and verification stations that are kept separate, i.e., two physical devices. A voter inserts an object called a token into the capture station to make ballot selections, and then takes the token object to the verification station to review and store his or her votes. Two records of the vote are created: one on the token object and one by the verification station.

6.0.1.3.1 Capture and Verification Stations

6.0.1.3.1.1 The verification station is able to add information to the token object but cannot change prior recorded information

Responsible Entity: voting system vendor
Process: voting

Discussion: This will need to be evaluated by attempting to find a way to allow writing during penetration testing.

6.0.1.3.1.2 The capture and verification stations do not permit any communications between them except via the token object.

Responsible Entity: voting system vendor
Process: voting

6.0.1.3.1.3 The verification station log all rejected votes, including the votes' precise contents and an identifier of the token object.

Responsible Entity: voting system vendor
Process: voting

Discussion: The voter could reject and essentially spoil his or her ballot. If the verification station shows ballot choices that are different from what was entered at the capture station, this could be an indication of a serious problem.

6.0.1.3.1.4 The capture and verification stations could be purchased from different manufacturers and should use different operating systems.

Responsible Entity: voting system vendor
Process: voting

Discussion: The greater the diversity between the systems, the less likely they could be compromised by the same threats, e.g., software viruses, or by a single conspiracy.

6.0.1.3.2 Data Formats for Token Objects

6.0.1.3.2.1 The format for data written to the token object should be specified and available for use without permission or licensing fees.

Responsible Entity: voting system vendor
Process: voting

6.0.1.3.2.2 The verification station verifies the correctness of the data on the token object according to the specification of its format and provides an indication of any errors to the voter.

Responsible Entity: voting system vendor
Process: voting

Discussion: The verification station needs to verify, in essence, that the data written to the token object was formatted according to the rules of the format's specification and reject ill-formatted data. It also checks that the votes are consistent with the voting instructions, e.g., "vote for one, vote for two."

6.0.1.3.2.3 The record on the token object is digitally signed using a private key known only to the vote capture station and whose public key is distributed in an authenticated way to auditing systems.

Responsible Entity: voting system vendor
Process: voting

6.0.1.3.2.4 The record created by the verification station is digitally signed using a private key known only to the verification station and whose public key is distributed in an authenticated way to auditing systems.

Responsible Entity: voting system vendor
Process: voting

6.0.1.3.2.5 The capture station associates with each record of voter choices a unique identifier that is capable of being used to identify the record uniquely and to identify its corresponding record created by the verification station.

Responsible Entity: voting system vendor
Process: voting

Discussion: The identifier should serve the purpose of uniquely identify the record so as to identify duplicates and/or for cross-checking two record types

6.0.1.3.2.6 The records from the verification station are randomly shuffled in memory and when exported so that the order of the records cannot be used to identify any voter.

Responsible Entity: voting system vendor
Process: voting

6.0.1.3.2.7 Rejected token objects are stored separately from accepted memory devices for later auditing.

Responsible Entity: voting system vendor
Process: voting

6.0.1.3.3 Storage and Communications of Records

6.0.1.3.3.1 The verification station exports its records of voter choices accompanied by a digital signature on the entire set of electronic records and their associated digital signatures.

Responsible Entity: voting system vendor
Process: voting

Discussion: This is necessary to determine if records are missing or substituted.

6.0.1.3.3.2 The token objects are carried in a physically secure way, using chain-of-custody mechanisms to ensure their integrity.

Responsible Entity: voting system vendor

Process: voting

6.0.1.3.3.3 The records from each station are randomly shuffled, so that an attacker learning the contents of those records at any point in the voting can learn nothing about the order of votes cast.

Responsible Entity: voting system vendor
Process: voting

6.0.1.4 Witness Independent Verification Systems (informative)

This section contains preliminary definitions Witness independent verification systems. They are consistent with the definition of independent verification systems from Section 6.0 and build on the core definitions from Section 6.0.1.2.

Witness independent verification systems are composed of two physically separate devices: the vote capture station that captures and stores records of voters' choices, and the witness device that captures voter verifications of the records at the vote recording station. Because there are two devices, a number of the definitions for split verification systems apply equally well to witness systems. Because the vote capture station is in essence a DRE (with or without VVPAT capability), a number of the definitions for VVPAT that are specific to DRE systems also apply to vote recording stations. A witness system fits somewhat loosely in the independent verification category because the voter performs only an indirect verification of ballot choices at the DRE and assumes that the witness device performs a second indirect verification. This assumption can be made only if the witness device is tested extensively for accuracy and reliability, and only if malfunctions in the device are made immediately obvious to voters and poll workers.

6.0.1.4.1 A witness device records only a voter's verification at a vote capture station and stores the record so that it can be used for audit and recounts as applicable.

Responsible Entity: voting system vendor
Process: voting

6.0.1.4.2 A witness device acts as a passive device that cannot perform any operation with respect to the capture station other than to capture the voter's ballot choices as the voter verifies them.

Responsible Entity: voting system vendor
Process: voting

Discussion: The witness device is synchronized with the voter verification of the ballot choices.

6.0.1.4.3 A witness device, if electrically connected to the capture station, is connected such that it can capture only the voter's verification of ballot choices.

Responsible Entity: voting system vendor
Process: voting

Discussion: For example, the witness device could be connected only to the display unit and not the capture station's memory or disk drive.

6.0.1.4.4 The capture station is not able to detect in its function whether a witness device is electrically connected or in operation.

Responsible Entity: voting system vendor
Process: voting

Discussion: If the witness device is connected to or attached electrically to the vote capture station, i.e., a DRE, the capture station is not able to determine or be aware in its function that a witness device is attached, other than its operating system would normally be able to determine that any device is attached to a hardware report under control of the operating system.

6.0.1.4.5 The witness device functions properly with most if not all electronic voting systems functioning as capture stations.

Responsible Entity: voting system vendor
Process: voting

Discussion: This is desirable but may possibly require some degree of openness in witness device specification so that voting system vendors could permit compatibility.

6.0.1.4.6 The witness device is not designed or built or manufactured by the same manufacturer of the capture station to which it is attached.

Responsible Entity: Testing Authorities
Process: voting

6.0.1.4.7 Because voters must trust that the witness device records their verifications accurately, assessments of its software and functionality are straightforward, readily performed, and include extensive evaluation and penetration testing above and beyond what may be performed on voting systems that do not contain witness devices.

Responsible Entity: Testing Authorities
Process: Pre-Voting

Discussion: Witness device manufacturers will need to document their systems extensively and subject them to highly stringent testing.

6.0.1.4.8 Because voters must trust that the witness device records their verifications accurately, the results of witness system assessments are made available publicly.

Responsible Entity: Testing Authorities
Process: Pre-Voting

6.0.1.4.9 A voter should be able to inspect the record of the voter's verification upon the voter's request.

Responsible Entity: voting system vendor
Process: voting

Discussion: It is desirable that a voter have some capability to verify that the witness device is operating as specified.

6.0.1.4.10 The witness device clearly indicates any malfunction in a way that is obvious to poll workers and voters.

Responsible Entity: voting system vendor, Voting Officials
Process: voting

Discussion: This requirement serves to ensure that voting cannot continue if the witness device is not operating or malfunctioning.

6.0.1.4.11 The records captured by the witness device are able to be used in highly accurate audits of the voting records captured and stored by the recording station.

Responsible Entity: voting system vendor
Process: voting

6.0.1.4.12 The records contain unique identifiers that correspond to records stored by the recording station.

Responsible Entity: voting system vendor
Process: voting

6.0.1.4.13 The records are digitally signed by the witness device so that the integrity and authenticity of its records can be verified in audits.

Responsible Entity: voting system vendor
Process: voting

6.0.1.4.14 A witness device is able to export its records in an open, nonproprietary format such that the records can be used in automated audits.

Responsible Entity: voting system vendor
Process: voting

6.0.1.4.15 The records are stored in the witness device and exported such that voter privacy is protected, e.g., by making the order of the records randomly determined.

Responsible Entity: voting system vendor
Process: voting

6.0.1.5 End to End (Cryptographic) Independent Verification Systems (Informative)

This section contains very preliminary definitions for End to End (or cryptographic-based) independent verification systems. They are consistent with the definition of independent verification systems from Section 6.0 and build on the core definitions from Section 6.0.1.2.

End to end voting systems use cryptographic mechanisms as a substitute for some physical, computer-security, or procedural mechanisms used to secure other voting systems. Some auditing procedures normally performed by election officials at the tabulation center can be done by voters or their designated representatives, using receipts issued by the voting system that work in conjunction with the cryptographic mechanisms. Several types of cryptographic voting schemes have been proposed or implemented, with varying properties. There are many cryptographic techniques (such as secure multiparty computation and homomorphic) that could be applied in novel ways within future voting systems.

6.0.1.5.1 End to end systems use cryptographic mechanisms as a substitute for some physical, computer security, and procedural mechanisms used to secure voting systems. These mechanisms can be used by a voter to verify that ballot choices were recorded correctly and counted in the election.

Responsible Entity: voting system vendor
Process: voting

Discussion: There are potentially many types of end to end systems that could perform a variety of different functions.

6.0.1.5.2 End to end systems record voters ballot choices at an electronic voting system and encrypt the records of votes for later counting by designated trustees.

Responsible Entity: voting system vendor
Process: voting

Discussion: The voting station would operate much as a DRE.

6.0.1.5.3 End to end systems produce a receipt that can be used by the voter in some process made available by election officials so that the voter may verify that the voter's ballot choices were recorded correctly and counted in the election.

Responsible Entity: voting system vendor
Process: voting

Discussion: The receipt could have a variety of different forms but likely would be printed on paper for the voter’s ease of handling.

6.0.1.5.4 No one trustee is able to decrypt the records; decryption of the records is performed by a process that involves multiple trustees.

Responsible Entity: voting system vendor, Voting System Officials
Process: Post-Voting

Discussion: For example, multiple keys could be combined to decrypt the records.

6.0.1.5.5 The receipt preserves voter privacy by not containing any information that can be used to show the voter’s choices.

Responsible Entity: voting system vendor
Process: voting

6.0.1.5.6 The process used to verify that ballot choices were recorded correctly or counted in the election preserves voter privacy by not revealing any information that can be used to show the voter's choices.

Responsible Entity: voting system vendor
Process: voting

6.0.1.5.7 End to end systems store backup records of voter's ballot choices that can be used in contingencies such as damage to or loss of its counted records.

Responsible Entity: voting system vendor
Process: voting

Discussion: This is necessary because the handling of the encrypted records requires the same chain of custody procedures as records produced by other voting systems and are thus subject to loss or damage. This could be paper for example.

6.0.1.5.8 The backup records contain unique identifiers that correspond to unique identifiers in its counted records, and the backup records are digitally signed so that they can be verified for their authenticity and integrity in audits.

Responsible Entity: voting system vendor
Process: voting

6.0.1.5.9 Cryptographic software in end to end systems is documented thoroughly and subject to extensive verification testing for correctness. The documentation includes extensive discussion of how cryptographic keys are to be generated, distributed, managed, used, certified, and destroyed.

Responsible Entity: Testing Authorities
Process: Pre-Voting

Discussion: The correctness of the system depends on the correctness of the cryptographic algorithms and their implementations. Thus, rigorous testing is necessary.

6.0.1.5.10 Vote capture stations used in end to end systems meet all security, usability, and accessibility requirements for similar stations in other voting systems.

Responsible Entity: voting system vendor
Process: voting

6.0.1.5.11 Reliability, usability, and accessibility requirements for printers in other voting systems apply as well to receipt printers used in end to end systems.

Responsible Entity: voting system vendor
Process: voting

6.0.1.5.12 Trustee systems are subject to the same evaluations and assessments as other voting systems.

Responsible Entity: voting system vendor
Process: Pre-Voting

6.0.1.5.13 Systems for verifying that voters' ballots were recorded properly and counted in the election are implemented in a robust secure manner.

Responsible Entity: voting System
Process: Post-voting

Discussion: Many of the cryptographic schemes have a "public append-only bulletin board" as a component; this is an important part of the system and needs to be implemented in a robust secure manner.

6.0.2 Requirements for Voter Verified Paper Audit Trails

This section contains requirements for voter verified paper audit trail systems. They build on the requirements for usability, accessibility, alternative languages, and privacy from Section 2.2.7 and are consistent with the definition of independent verification systems from Section 6.0.

VVPAT is a form of direct independent verification systems. A future version of the section will contain additional requirements for other types of directly verified systems such as for some types of optical scan.

6.0.2.1 The voting station shall print and display a paper record of the voter's ballot choices prior to the voter making the ballot choices final.

Responsible Entity: voting system vendor
Process: voting

Discussion: This is the basic requirement for VVPAT capability. It requires that the paper record be created as a distinct representation of the voter's ballot choices. It requires that the paper record contain the same information as contained in the electronic record and be suitable for use in audits and recounts of the election and of the voting station's electronic records. Thus, either the paper or electronic record could be used as the ballot of record for the election.

6.0.2.1.1 The paper records shall constitute a complete record of ballot choices that can be used in audits of the accuracy of the voting station's electronic records, in audits of the election results, and in full recounts.

Responsible Entity: voting system vendor
Process: voting

Discussion: This requirement exists to make clear that it shall be possible to use the paper record for audits of the voting station's accuracy in recording voter's ballot choices, as well as usable for election audits (such as mandatory 1% recounts). The paper record shall also be suitable for use in full manual recounts of the election.

6.0.2.1.2 The paper record shall contain all information stored in the electronic record.

Responsible Entity: voting system vendor
Process: voting

Discussion: The electronic record cannot hide any information related to ballot choices; all information relating to ballot choices must be equally present in both records. The electronic record may have other items that don't necessarily need to be on the paper record, such as digital signature information.

6.0.2.2 All usability requirements from section 2.2.7 shall apply to voting stations with VVPAT.

Responsible Entity: voting system vendor
Process: voting

Discussion: The requirements in this section are in addition to those requirements from Section 2.2.7. They mandate that the paper record be formatted and displayed so that the voter is able to verify his or her votes with maximum reasonable ease and satisfaction, and that instructions be provided to the voter to handle all relevant aspects of the voter verification.

6.0.2.2.1 The voting station shall be capable of showing the information on the paper in a font size of 3.0 mm, and should be capable of showing the information in at least two font ranges, a) 3.0-4.0 mm and b) 6.3-9.0 mm, under control of the voter.

Responsible Entity: voting system vendor
Process: voting

Discussion: In keeping with requirements in Section 2.2.7, the paper record should use the same font sizes as displayed by the voting station, but at least be capable of 3.0 mm. While larger font sizes may assist most voters with poor vision, certain disabilities such as tunnel vision are best addressed by smaller font sizes.

6.0.2.2.2 The paper and electronic records shall be presented so as to allow for easy, simultaneous comparison.

Responsible Entity: voting system vendor
Process: voting

Discussion: If the records are similar in design and layout as much as possible, this will assist voters in comparing the records.

6.0.2.2.2.1 The paper and electronic records shall be positioned so that voters can, at the same posture, easily read and compare the two records.

Responsible Entity: voting system vendor
Process: voting

Discussion: The voter should not have to shift positions when comparing the records.

6.0.2.2.2.2 If the paper record cannot be displayed in its entirety, a means for moving the paper to show all paper record contents shall be provided and shall be clearly indicated.

Responsible Entity: voting system vendor
Process: voting

Discussion: Possible solutions include scrolling the paper or printing a new sheet of paper.

6.0.2.2.2.3 If the paper record cannot be displayed in its entirety, each page of the record shall be numbered and shall include the total count of pages for the record.

Responsible Entity: voting system vendor
Process: voting

Discussion: Possible numbering schemes include "page X of Y."

6.0.2.2.3 There shall be instructions for performing the verification process made available to the voter in a location on the voting station.

Responsible Entity: voting system vendor
Process: voting

6.0.2.3 All accessibility requirements from section 2.2.4 shall apply to voting stations with VVPAT.

Responsible Entity: voting system vendor
Process: voting

Discussion: Accessibility and alternative language requirements from Sections 2.2.7.1 and 2.2.7.2 apply generically to voting stations with VVPAT; requirements in this section are in addition to those requirements from Section 2.2.7. They make explicit that an accessible vote verification procedure for voters be provided at voting sites, including voters with disabilities, Limited English Proficiency (LEP), and voters with Native American and Alaska Native languages that are not written.

6.0.2.3.1 The voting station shall display, print, and store a paper record in any of the alternative languages chosen for making ballot selections.

Responsible Entity: voting system vendor
Process: voting

Discussion: For the purposes of voter privacy, it must not be possible to identify voters based on their use of alternative languages. Requirement 6.0.2.5.3 addresses this issue.

6.0.2.3.1.1 For the purposes of auditing, candidate names on the records shall be in English.

Responsible Entity: voting system vendor
Process: voting

Discussion: This requirement is included to assist manual auditing of the paper records.

6.0.2.3.1.2 Other markings not related to ballot selection on the paper ballot shall be in English.

Responsible Entity: voting system vendor
Process: voting

Discussion: Other markings may include designations of the precinct and the election.

6.0.2.3.2 If the normal procedure includes VVPAT, the accessible voting station shall provide features that enable voters who are blind to perform this verification.

Responsible Entity: voting system vendor
Process: voting

Discussion: This requirement is repeated from Section 2.2.7 and included here for emphasis.

6.0.2.4 The voting station shall allow the voter to approve or spoil the paper record.

Responsible Entity: voting system vendor
Process: voting

Discussion: The voting station cannot create an electronic record without its corresponding paper record. It requires that the voting station mark the electronic record as accepted or spoiled in the voter's presence, and if spoiled, the corresponding electronic record be marked as spoiled and be preserved. It requires that the voting station display a warning message when a spoil limit is reached.

6.0.2.4.1 The voting station shall, in the presence of the voter, mark the paper record as being accepted by the voter or spoiled.

Responsible Entity: voting system vendor
Process: voting

Discussion: If a paper record is marked as spoiled, then the corresponding electronic record is presented to the voter for update.

6.0.2.4.2 The voting station shall mark and preserve electronic and paper records that have been spoiled.

Responsible Entity: voting system vendor
Process: voting

Discussion: For the purposes of reconciliation of records, spoiled records should be retained and analyzed.

6.0.2.4.2.1 Following the close of polls, a means shall be provided to reconcile the number of spoiled paper records with the number of occurrences of spoiled electronic records, and procedures shall be in place to address any discrepancies.

Responsible Entity: voting system vendor, voting official
Process: post-voting

6.0.2.4.2.2 Prior to the maximum number of spoiled ballots occurring, the voting station shall display a warning message to the voter indicating that the voter may spoil only one more ballot.

Responsible Entity: voting system vendor
Process: voting

Discussion: The maximum number of spoiled ballots varies from state to state.

6.0.2.4.2.3 If the maximum number of spoiled ballots occurs, procedures shall be in place to permit the voter to otherwise cast a ballot.

Responsible Entity: voting system vendor, voting official
Process: voting

Discussion: Possible solutions include using other equipment, using a paper ballot, or accepting the last ballot cast.

6.0.2.4.3 In case of conditions that prevent voter review of the paper record, there shall be a means for the voter to notify an election official.

Responsible Entity: voting official
Process: voting

6.0.2.4.3.1 Conditions that prevent voter review of the paper record that are detectable to the voting station shall cause an error message to be displayed and shall prevent recording of the electronic record.

Responsible Entity: voting system vendor
Process: voting

6.0.2.4.4 Procedures by which election officials can be notified and prescribed actions can be taken to address discrepancies if a voter indicates that the electronic and paper records do not match shall be documented.

Responsible Entity: voting system vendor, voting official
Process: voting

Discussion: If the records do not match, a potentially serious error has occurred. Election officials must first verify that the records do not match and then take appropriate actions such as removing the voting station from service and quarantining its records for later analysis.

6.0.2.4.5 The voting station should not record the electronic record as being approved by the voter until the paper record has been stored.

Responsible Entity: voting system vendor
Process: voting

Discussion: In general it is better not to record any record as being approved by the voter until all records are approved by the voter.

6.0.2.4.6 There shall be a capability to address situations in which an electronic or paper record has been recorded, approved, and stored without the intention of the voter.

Responsible Entity: voting system vendor
Process: voting

Discussion: This may be due to conditions such as errors at the voting station or mistakes by the voter.

6.0.2.4.6.1 The capability shall include the option of spoiling the records.

Responsible Entity: voting system vendor
Process: voting

6.0.2.4.7 Vendor documentation shall include procedures for returning a voting station to correct operation after a voter has used it incompletely or incorrectly; this procedure shall not cause discrepancies between the tallies of the electronic and paper records.

Responsible Entity: voting system vendor
Process: voting

6.0.2.5 The voter's privacy and anonymity shall be preserved during the process of recording, verifying, and auditing ballot choices.

Responsible Entity: voting system vendor
Process: voting

Discussion: Privacy requirements from section 2.2.7 apply to voting stations with VVPAT; requirements in this section are in addition to those requirements from Section 2.2.7. They require that the voter's privacy be maintained during the verification step, including requirements that the paper ballot contain no human or machine-readable markings that could identify the voter and that the paper and electronic records be stored in ways that preserve the privacy and anonymity of the voter.

6.0.2.5.1 The privacy and anonymity of the voter's verification of his or her ballot choices on the electronic and paper records shall be maintained.

Responsible Entity: voting system vendor
Process: voting

6.0.2.5.2 The electronic and paper records shall be created and stored in ways that preserve the privacy and anonymity of the voter.

Responsible Entity: voting system vendor
Process: voting

Discussion: This can be accomplished in various ways including shuffling the order of the records or other methods to separate the order of stored records.

6.0.2.5.3 The privacy and anonymity of voters whose paper records contain any of the alternative languages chosen for making ballot selections shall be maintained.

Responsible Entity: voting system vendor, voting official
Process: voting

Discussion: One method for accomplishing this is to ensure that no less than five voters use any of the alternative languages for their ballot selections.

6.0.2.5.4 The voter shall not be able to leave the voting area with the paper record if the information on the paper record can reveal the voter's choices.

Responsible Entity: voting system vendor, Voting Official
Process: voting

6.0.2.5.5 Information for the purposes of auditing the electronic or paper records that may permit a voter to reveal his or her ballot choices shall be displayed so as not to be memorable by the voter.

Responsible Entity: voting system vendor
Process: voting

Discussion: Unique identifiers on the paper record should be displayed or formatted in such a way that they are not memorable to voters, such as by obscuring them in other characters or in a barcode.

6.0.2.5.6 The privacy and anonymity of voters unable to manually handle paper and who use an accessible voting station that requires manual storage of the paper record into a ballot box shall be maintained.

Responsible Entity: voting system vendor
Process: voting

6.0.2.6 The voting station's ballot records shall be structured and contain information so as to support highly precise audits of their accuracy.

Responsible Entity: voting system vendor
Process: voting

Discussion: It requires that electronic records and paper records contain election precinct information, information to link the paper record to its corresponding electronic record, and information identifying the voting station. It requires that the electronic records be maintained in a format that can be exported to a different computer, i.e., a personal computer, and that the format be well-documented to support analysis of the records.

6.0.2.6.1 All cryptographic software in the voting station shall have been approved by the U.S. Government's Crypto Module Validation Program (CMVP) as applicable.

Responsible Entity: voting system vendor
Process: voting

Discussion: The voting station may use cryptographic software for a number of different purposes, including calculating checksums, encrypting records, authentication, generating random numbers, and for digital signatures. This software shall be reviewed and approved by the Crypto Module Validation Program. There may be cryptographic voting schemes where the cryptographic algorithms used are necessarily different from any algorithms that have approved CMVP implementations, thus CMVP approved software should be used where feasible. The CMVP web site is http://csrc.nist.gov/cryptval.

6.0.2.6.2 The electronic and paper records shall include information about the election.

Responsible Entity: voting system vendor
Process: voting

6.0.2.6.2.1 The records shall include an identification of the voting site/precinct.

Responsible Entity: voting system vendor

Process: voting

Discussion: If the voting site and precinct are different, both should be included.

6.0.2.6.2.2 The records shall include information identifying whether the balloting is provisional, early, or on Election Day, and information that identifies the ballot style in use.

Responsible Entity: voting system vendor
Process: voting

6.0.2.6.2.3 The records shall include a voting session identifier that is generated when the voting station is placed in voting mode and that can be used to identify the records as being created during that voting session.

Responsible Entity: voting system vendor
Process: voting

Discussion: If there are several voting sessions on the same voting station on the same day, the voting session identifiers must be different. They should be generated from a random number generator.

6.0.2.6.3 The electronic and paper records shall be linked by including a unique identifier within each record that can be used to identify each record uniquely and each record's corresponding record.

Responsible Entity: voting system vendor
Process: voting

Discussion: The identifier should serve the purpose of uniquely identify the record so as to identify duplicates and/or for cross-checking two record types

6.0.2.6.4 The voting station shall generate and store a digital signature for each electronic record.

Responsible Entity: voting system vendor
Process: voting

6.0.2.6.5 The electronic records shall be able to be exported for auditing or analysis on standards based and/or COTS information technology computing platforms.

Responsible Entity: voting system vendor
Process: voting

6.0.2.6.5.1 The exported electronic records shall be in an open, non-proprietary format and should preferentially be in a format that is commonly used by electronic voting system manufacturers.

Responsible Entity: voting system vendor
Process: voting

Discussion: The format must be open and it is best that all electronic records, regardless of manufacture, use the same format, e.g., OASIS EML.

6.0.2.6.5.2 The voting station shall export the records accompanied by a digital signature of the collection of records, which shall be calculated on the entire set of electronic records and their associated digital signatures.

Responsible Entity: voting system vendor
Process: voting

Discussion: This is necessary to determine if records are missing or substituted.

6.0.2.6.5.3 The voting system vendor shall provide documentation as to the structure of the exported records and how they shall be read and processed by software.

Responsible Entity: voting system vendor
Process: voting

6.0.2.6.5.4 The voting station manufacturer shall provide a software program that will display the exported records and that may include other capabilities such as providing vote tallies and indications of undervotes.

Responsible Entity: voting system vendor
Process: voting

6.0.2.6.6 The paper records should be created in a format that may be made available across different manufacturers of electronic voting systems.

Responsible Entity: voting system vendor
Process: voting

Discussion: Future standards may require some commonality in the format of paper records.

6.0.2.6.7 The paper record shall be created such that its contents are machine-readable.

Responsible Entity: voting system vendor
Process: voting

Discussion: This can be done by using specific OCR fonts.

6.0.2.6.7.1 The paper record should contain error correcting codes for the purposes of detecting read errors and for preventing other markings on the paper record to be misinterpreted when machine reading the paper record.

Responsible Entity: voting system vendor
Process: voting

Discussion: This requirement is not mandatory if, for example, a state prohibits non-human-readable information on the paper record. This requirement serves the purpose of detecting scanning errors and preventing stray or deliberate markings on the paper from being interpreted as valid data.

6.0.2.6.8 Any automatic accumulation of electronic or paper records shall be capable of detecting and discarding duplicate copies of the records.

Responsible Entity: voting system vendor
Process: voting

6.0.2.6.9 The voting station should be able to print a barcode with each paper record to contain the human readable contents of the paper record and digital signature information.

Responsible Entity: voting system vendor
Process: voting

Discussion: This requirement is not mandatory if, for example, a state prohibits non-human-readable information on the paper record.

6.0.2.6.9.1 The barcode shall use an industry-standard format and shall be able to be read using readily available commercial technology.

Responsible Entity: voting system vendor
Process: voting

Discussion: Examples of such codes are Maxi Code or PDF417.

6.0.2.6.9.2 The bar code shall contain the digital signature of the paper record's corresponding electronic record.

Responsible Entity: voting system vendor
Process: voting

6.0.2.6.9.3 The barcode shall not contain any information other than the paper record’s human readable content and digital signature information.

Responsible Entity: voting system vendor
Process: voting

6.0.2.6.9.4 A scanner for reading and displaying the bar code shall be made available to voters at their request.

Responsible Entity: voting system vendor
Process: voting

6.0.2.6.10 The voting system vendor shall provide full documentation of procedures for exporting its electronic records and reconciling its electronic records with its paper records.

Responsible Entity: voting system vendor
Process: voting

6.0.2.7 The voting station equipment shall be secure, reliable, and easily maintained.

Responsible Entity: voting system vendor
Process: voting

Discussion: It specifies requirements for high reliability, maintenance, and security of the voting station's equipment including printer, display and ballot box. It requires that adequate supplies be maintained. It requires that appropriate procedures and environmental controls be used to maintain supplies and paper records.

6.0.2.7.1 The voting station shall be physically secure from tampering, including intentional damage.

Responsible Entity: voting system vendor, voting official
Process: voting

6.0.2.7.1.1 The voting station shall communicate with its printers over a standard, publicly documented printer port using a standard communication protocol.

Responsible Entity: voting system vendor
Process: voting

Discussion: Using a standard, publicly documented printer protocol assists in security evaluations of its software.

6.0.2.7.1.2 The paper path between the printing, viewing and storage of the paper record shall be protected and sealed from access except by authorized election officials as specified by local law.

Responsible Entity: voting system vendor
Process: voting

6.0.2.7.1.3 The printer shall not be permitted to communicate with any other system or machine other than the single voting machine to which it is connected.

Responsible Entity: voting system vendor
Process: voting

6.0.2.7.1.4 The printer shall only be able to function as a printer; it cannot spool information or contain any services (e.g., provide copier or fax functions) or network capability.

Responsible Entity: voting system vendor
Process: voting

6.0.2.7.1.5 Printer access to replace consumables such as ink or paper shall only be granted if it does not compromise the sealed printer paper path.

Responsible Entity: voting system vendor
Process: voting

6.0.2.7.1.6 The ballot box storing the paper records shall be sealed and secured and no access shall be provided to polling place workers.

Responsible Entity: voting system vendor
Process: voting

6.0.2.7.1.7 Tamper-evident seals or physical security measures shall protect the connection between the printer and the voting machine, so that the connection cannot be broken or interfered with without leaving extensive and obvious evidence.

Responsible Entity: voting system vendor
Process: voting

6.0.2.7.2 The voting station's printer shall be highly reliable, and easily maintained.

Responsible Entity: voting system vendor
Process: voting

6.0.2.7.2.1 The voting station should include a printer port to which a commercial off-the-shelf printer could be attached for the purposes of printing paper records and any additional records.

Responsible Entity: voting system vendor
Process: voting

Discussion: This is not mandatory; however it would be useful to be able to attach a secondary printer if needed

6.0.2.7.2.2 The voting station shall detect errors and malfunctions such as paper jams or low supplies of consumables such as paper and ink that may prevent paper records from being correctly displayed or printed or stored.

Responsible Entity: voting system vendor
Process: voting

Discussion: This could be accomplished in a variety of different ways, for example, a printer that is out of paper or jammed could issue audible alarms, with the alarm different for each condition.

6.0.2.7.2.3 If errors or malfunctions occur, the voting station shall suspend voting operations and shall present a clear indication to the voter and election workers of the malfunctions.

Responsible Entity: voting system vendor
Process: voting

Discussion: The voting station should not record votes if errors or malfunctions occur.

6.0.2.7.2.4 Printing devices should contain paper and ink of sufficient capacity so as not to require reloading or opening equipment covers or enclosures and circumvention of security features, or reloading shall be able to be accomplished with minimal disruption to voting and without circumvention of security features such as seals.

Responsible Entity: voting system vendor
Process: voting

6.0.2.7.2.5 There shall be adequate supplies of consumable items such as paper and printer ink on hand to operate from opening to closing of polls.

Responsible Entity: voting officials
Process: voting

6.0.2.7.2.6 Printer consumables shall be stored within the temperature and humidity ranges specified by the manufacturer and shall be stored in approved containers to protect them from sustaining any damage.

Responsible Entity: voting system vendor, voting officials
Process: pre-voting/post-voting

6.0.2.7.2.7 A sufficient number of replacement printers shall be available at each polling location.

Responsible Entity: voting system vendor
Process: voting

Discussion: It may be best for the vendor to recommend a sufficient number based on the total number of voting stations. At least one replacement printer should be available.

6.0.2.7.2.8 Vendor documentation shall include procedures for investigating and resolving malfunctions including but not limited to misreporting of votes, unreadable paper records, paper jams, low ink, miss feeds, and power failures.

Responsible Entity: voting system vendor
Process: voting

6.0.2.7.2.9 Vendor documentation shall include procedures for ensuring, in the case of malfunctions, that electronic and paper records are correctly recorded and stored.

Responsible Entity: voting system vendor
Process: voting

6.0.2.7.3 Protective coverings intended to be transparent on voting station devices shall be maintainable via a predefined cleaning process. If the coverings become damaged such that they obscure the paper record, they shall be replaced.

Responsible Entity: voting system vendor

Process: voting

6.0.2.7.4 The paper record shall be sturdy, clean, and of sufficient durability to be used for manual auditing, machine auditing, and recounts conducted manually and via machine reading equipment.

Responsible Entity: voting system vendor
Process: voting

6.0.2.7.4.1 The paper record shall be able to be stored without degradation for 22 months within the temperature and humidity ranges specified by the manufacturer.

Responsible Entity: voting system vendor
Process: voting

6.0.2.7.4.2 The paper record shall be stored in an approved container that protects it from sustaining bends, creases and edge dents.

Responsible Entity: voting system vendor, voting officials
Process: voting

6.0.3 Wireless Requirements

This section provides wireless requirements for implementing and using wireless capabilities within a voting system. These requirements reduce, not eliminate, the risk of using wireless communications for voting systems.

Wireless is defined as any means of communication that occurs without wires. This covers the entire electromagnetic spectrum, and is not limited to a subset of the spectrum (e.g., radio frequency, infrared, or microwave) or to a specific wireless technology (e.g., IEEE Std. 802.11). This definition of wireless includes audible and visible light. Wireless communications are bi-directional. That is the wireless communicating devices both send and receive data, even if logically the concerned data (e.g., precinct counts) is only unidirectional. Since the wireless communications path on which the signals travel is via the air and not via a wire or cable, other devices can receive the wireless signals (e.g., voting data) without requiring a physical connection. Some of the wireless communications paths (i.e., signals) are weakened by walls and distance, but are not stopped. This permits eavesdropping from a distance and permits an attacker to transmit wireless signals (e.g., interference or intrusive data) from a distance. In many cases the wireless signals cannot be seen, heard, or felt, thus making the presence of wireless communication hard to determine by the human senses. Also the generation of some of these wireless signals may cause additional electromagnetic stresses that could impact voting system accuracy. It is to these issues (i.e., controlling and identifying usage, protecting the transmitted data and path, and protecting the system), that these requirements are made.

Inclusion of wireless communications into a voting system negates the ability to physically secure the system (e.g., physical locate the system in a restricted area). Even if all of the following requirements are implemented, the voting system is still not as secure as if wireless communications were not present and used. In other words, the use of wireless technology introduces risk and should be approached with caution.

The requirements that are applicable to all types of wireless communications are presented, followed by requirements that are applicable to a specific part of the electromagnetic spectrum (e.g., audible, radio frequency, and infrared). These latter requirements only apply to systems using this part of the spectrum.

6.0.3.1 At a minimum wireless communications shall meet the requirements listed in Volume I, section 5, "Telecommunications."

Responsible Entity: voting system vendor
Process: pre-voting, voting, post-voting

6.0.3.2 Controlling usage

6.0.3.2.1 If wireless communications are used in a voting system, then the vendor shall supply documentation describing how to use all aspects of wireless communications in a secure manner.

Responsible Entity: voting system vendor
Process: pre-voting, voting, post-voting

6.0.3.2.1.1 This documentation shall include:
-- a careful and complete description of the uses of wireless in the voting system including descriptions of the data elements and signals that are to be carried by the wireless mechanism,
-- a careful and complete description of the vulnerabilities associated with this proposed use of wireless, including vulnerabilities deriving from the insertion, deletion, modification, capture, or suppression of wireless messages,
-- a careful and complete description of the techniques used to mitigate the risks associated with the described vulnerabilities including techniques used by the vendor to ensure that wireless cannot send or receive messages other than those situations specified in the documentation. Cryptographic techniques shall be carefully and fully described, including a description of cryptographic key generation, management, use, certification, and destruction.
-- a rationale for the inclusion of wireless in the proposed voting system, based on a careful and complete description of the perceived advantages and disadvantages of using wireless for the desired functionality compared to using a non-wireless approaches.

Responsible Entity: voting system vendor
Process: pre-voting

Discussion: In general, convenience is not a sufficiently compelling reason, on its own, to justify the inclusion of wireless in a voting system. If convenience is cited as an advantage of wireless, it must be balanced against the difficulty of working with cryptographic keys.

6.0.3.2.1.2 The voting official shall have appropriate procedures for cryptographic key management.

Responsible Entity: voting official
Process: pre-voting

6.0.3.2.1.3 The details of all cryptographic protocols used for wireless including the specific features and data shall be documented.

Responsible Entity: voting system vendor
Process: pre-voting

6.0.3.2.1.4 The wireless documentation shall be closely reviewed for accuracy, completeness, and correctness.

Responsible Entity: testing authority
Process: pre-voting

6.0.3.2.1.4.1 This review shall be either done through an open and public review or by a subject area recognized expert.

Responsible Entity: testing
Process: pre-voting

6.0.3.2.1.5 There shall be no undocumented use of the wireless capability, nor shall there be any use of the wireless capability that is not entirely controlled by the voting official.

Responsible Entity: testing authority
Process: pre-voting

Discussion: This shall be tested by reviewing all of the software, hardware, and documentation and by testing the status of wireless activity during all phases of testing.

6.0.3.2.2 If a voting system includes wireless capabilities, then the voting system shall be able to accomplish the same function if wireless capabilities are not available due to an error or no service.

Responsible Entity: voting system vendor
Process: pre-voting, voting, post-voting

6.0.3.2.2.1 The vendor shall provide documentation how to accomplish these functions when wireless is not available.

Responsible Entity: voting system vendor

Process: pre-voting, voting

6.0.3.2.3 The system shall be designed and configured such that it is not vulnerable to a single point of failure using wireless communications that causes a total loss of any of the other voting capabilities.

Responsible Entity: voting system vendor
Process: pre-voting, voting, or post-voting

Discussion: Rewritten from Volume 1, section 5.2.6 Integrity item c)

6.0.3.2.4 If a voting system includes wireless capabilities, then the system shall have the capability to be able to turn on the wireless capability when it is to be used and to turn off the wireless capability when the wireless capability is not in use.

Responsible Entity: voting system vendor
Process: pre-voting, voting, post-voting

6.0.3.2.4.1 The voting official shall ensure that the wireless capabilities are active only when needed.

Responsible Entity: voting official
Process: pre-voting, voting, post-voting

6.0.3.2.5 If a voting system includes wireless capabilities, then the system shall not activate the wireless capabilities without confirmation from a voting official.

Responsible Entity: voting system vendor
Process: pre-voting, voting, post-voting.

6.0.3.2.6 Radio frequencies

6.0.3.2.6.1 To reduce the potential for unintended interference, the wireless communications (radio frequencies) chosen for use in a voting system should not use radio frequencies that are widely used for non-voting systems devices that may be present in or near the expected place (e.g., polling place) of wireless usage.

Responsible Entity: voting official
Process: pre-voting, voting, post-voting.

6.0.3.2.6.2 To reduce the potential for intentional interference and to decrease the amount of the intended radiation, the wireless communications (radio frequencies) used should have the capability to control the signal strength. The range of control, if any, will be determined by the specific wireless technology used.

Responsible Entity: voting system vendor
Process: pre-voting, voting, post-voting.

6.0.3.2.6.3 A radio emissions site test should be conducted at any location (e.g., polling place) where the wireless voting system is to be used to determine the current level of interference, as well as to determine the projected level of the voting system(s) wireless emissions.

Responsible Entity: voting official
Process: pre-voting, voting, post-voting

Discussion: The test would need to occur at times near each planned wireless usage, since the availability and usage of wireless communications in non-voting systems change quickly. This radio emissions site test may be used to determine other nearby wireless non-voting systems that could potentially interfere with the voting system.

6.0.3.3 Identifying usage

Since there are a wide variety of wireless technologies (both standard and proprietary) and differing physical properties of wireless signals, it is important to identify some of the characteristics of the wireless technologies used in the voting system.

6.0.3.3.1 If a voting system provides wireless communications capabilities, then there shall be a method for determining the existence of the wireless communications capabilities.

Responsible Entity: voting system vendor
Process: pre-voting, voting, post-voting

6.0.3.3.2 If a voting system provides wireless communications capabilities, then there shall be an indication that permits determining when the wireless communications (e.g., radio frequencies) capability is active.

Responsible Entity: voting system vendor
Process: pre-voting, voting, post-voting

6.0.3.3.2.1 The indication should be visual.

Responsible Entity: voting system vendor
Process: pre-voting, voting, post-voting

6.0.3.3.3 If a voting system provides wireless communications capabilities, then there shall be a label (or at the least in the voting system's documentation) that identifies the wireless communications (e.g., radio frequencies) used.

Responsible Entity: voting system vendor
Process: pre-voting, voting, post-voting

6.0.3.4 Protecting the transmitted data

The transmitted data, especially via wireless communications, needs to be protected to ensure confidentiality (e.g., if individual ballots, vote counts, or passwords are transmitted) and integrity (e.g., if ballot definitions are transmitted).
Some examples of election information to be protected are

- ballot definitions,
- ballot instructions (audio),
- voting device counts,
- precinct counts,
- opening of poll signal, and
- closing of poll signal.

Some examples of information that is not specifically election information to be protected are

- protocol messages,
- address or device identification information, and
- passwords.

Since radio frequency wireless signals radiate in all directions and pass through most construction material, the reception of the wireless signals by any one is assumed to be easy. Unlike the radio frequency wireless signals, infrared signals are line of sight and do not pass through most construction materials. To a lesser extent these infrared signals can still be received by other devices that are in the line of sight. Thus to protect the privacy or confidentiality of the information, encryption is required. Similarly wireless signals can also be easily transmitted by others in order to create unwanted signals.

[Rewritten from Volume 1, section 6.5.3.]

6.0.3.4.1 All information transmitted via wireless communications shall be encrypted, with the exception of wireless coupling, to protect against eavesdropping and data manipulation including modification, insertion, and deletion.

Responsible Entity: voting system vendor, voting official
Process: pre-voting, voting, post-voting

6.0.3.4.1.1 The encryption shall be as defined in Federal Information Processing Standards (FIPS) 197, "Advanced Encryption Standard (AES)".

Responsible Entity: voting system vendor, voting official
Process: pre-voting, voting, post-voting

6.0.3.4.1.1.1 The cryptographic modules used shall comply with FIPS 140-2, Security requirements for Cryptographic Modules.

Responsible Entity: voting system vendor, voting official, testing entity
Process: pre-voting

6.0.3.4.1.2 The capability to transmit information via wireless without being encrypted shall not be present.

Responsible Entity: voting system vendor
Process: pre-voting, voting, post-voting

6.0.3.4.1.2.1 If wireless communication (audible) is used, and if the receiver of the wireless transmission is the human ear, then the information shall not be encrypted (i.e., this specifically covers the case of the wireless coupling for assistive devices used by people who are hard of hearing). [See Volume I, section 2.2.7.2 DRE standards item c)]

Responsible Entity: voting system vendor
Process: pre-voting, voting, post-voting

6.0.3.5 Protecting the wireless path

With the exception of wireless communications using audible and infrared, it is technically infeasible to use physical means to prevent denial of service attacks (DoS). If wireless communications are used, in order to minimize the risk of a denial of service (DoS) attack:

6.0.3.5.1 The voting system shall be able to function properly since the denial of service (DoS) attack could last for an infinite amount of time;

Responsible Entity: voting system vendor
Process: pre-voting, voting, post voting

6.0.3.5.2 The voting system shall function as if the wireless capability were never available for use; and

Responsible Entity: voting system vendor
Process: pre-voting, voting, post voting

6.0.3.5.3 Other procedures or capabilities shall exist to accomplish the same function that the wireless communications capability would have done.

Responsible Entity: voting system vendor
Process: pre-voting, voting, post voting

6.0.3.5.4 The wireless (audible) path shall be protected or shielded.

Responsible Entity: voting system vendor, voting official
Process: voting

Discussion: Protecting the audible path is a trade off between the high volume level from a speaker necessary for an individual to hear with the low volume level necessary to keep others from hearing, as well as protecting from interference (i.e., noise) from the polling place, voting station, or voting environment. The same is true for the audible path if a voter's speech is to be captured by the voting device. This wireless communication's path protection is necessary to protect privacy. Some audio head sets may already satisfy this requirement for the hearing part, while a sound proof voting booth may be necessary in some other cases (e.g., voice recordings).

6.0.3.5.5 Infrared

Since infrared has the line-of-sight (LoS) property, securing the wireless path can be accomplished by shielding the path between the wireless communicating devices with an opaque enclosure. However this is only practical for short distances. Also this type of shielding is needed to prevent accidental damage to the eyes by the infrared signal.

6.0.3.5.5.1 The shielding shall be strong enough to prevent escape of the voting system's signal, as well as strong enough to prevent infrared saturation jamming.

Responsible Entity: voting system vendor
Process: pre-voting, voting, post-voting

6.0.3.6 Protecting the voting system from a wireless-based attack

The security of the wireless voting systems is as important, if not more so, than the information transmitted. If a voting system becomes compromised, there is no telling

what harm may result, until the compromise is discovered and an investigation is conducted in order to determine the extent of the damage.

Physical security measures [Volume I, section 6.3] to prohibit access to a voting system are not possible when using a wireless (e.g., radio frequency) communications interface. This is similar to when access is through a telecommunications interface, but it is worsened by the fact that there is no wire (physical communication path) to physically secure and by the various physical properties of the electromagnetic spectrum used.

This section covers the applicable overall system capabilities section (i.e., security, accuracy, error recovery, integrity, and system audit), as well as authentication. The overall system capabilities are not exempt for wireless communications just because wireless is not mentioned there. Those requirements are re-affirmed here.

6.0.3.6.1 The security requirements listed in Volume I, section 2.2.1 shall be applicable to systems with wireless communications.

Responsible Entity: voting system vendor
Process: pre-voting, voting, post-voting

6.0.3.6.2 The accuracy requirements listed in Volume I, section 2.2.2 shall be applicable to systems with wireless communications.

Responsible Entity: voting system vendor
Process: pre-voting, voting, post-voting

6.0.3.6.2.1 The use of wireless communications that may cause impact to the system's accuracy through electromagnetic stresses is prohibited.

Responsible Entity: voting system vendor
Process: pre-voting, voting, post-voting

6.0.3.6.3 The error recovery requirements listed in Volume I, section 2.2.3, shall be applicable to systems with wireless communications.

Responsible Entity: voting system vendor
Process: pre-voting, voting, post-voting

6.0.3.6.4 All wireless communications actions shall be logged.

Responsible Entity: voting system vendor, voting official
Process: pre-voting, voting, post-voting

Discussion: As a way of monitoring the wireless communications a log of important information is maintained. This is to ensure that the wireless

communications is only used by authorized users with authorized devices to authorized access to authorized services, or at least see when it was not. This relates to the system audit requirements (See. Volume I, section 2.2.5) and integrity (See Volume I, section 2.2.4), if wireless is used.

6.0.3.6.4.1 The log shall contain at least the following entries. – times wireless activated and deactivated, services accessed, identification of device to which data was transmitted to or received from, identification of authorized user, successful and unsuccessful attempts to access wireless communications or service.

Responsible Entity: voting system vendor, voting official
Process: pre-voting, voting, post-voting

Discussion: Other information like the number of frames or packets transmitted or received at various logical layers may be useful, but is dependent on the wireless technology used.

6.0.3.6.5 Authentication

Wireless communications opens a door or a window of opportunity, which now must be secured to permit only authorized users using authorized devices authorized access to obtain authorized services.

6.0.3.6.5.1 Device authentication shall occur before any access to or services from the voting system are granted through wireless communications.

Responsible Entity: voting system vendor
Process: pre-voting, voting, post-voting

6.0.3.6.5.2 User authentication shall be at least level 2 as per NIST Special Publication 800-63 Version 1.0.1, “Electronic Authentication Guideline”

Responsible Entity: voting system vendor
Process: pre-voting, voting, post-voting

6.0.4 Distribution of Voting System Software and Setup Validation

This section specifies requirements for the distribution of voting system software and the setup validation performed on voting system equipment. These requirements are applicable to voting systems that have completed qualification testing. The goal of the software distribution requirements is to ensure that the correct voting system software has been distributed without modification. The goal of setup validation requirements, including requirements for verifying the presence of qualified software and the absence of other software, is to ensure that voting system equipment is in a proper initial state before being used.

In general, a voting system can be considered to be composed of multiple other systems including polling place systems, central counting/aggregation systems, and election management systems. These other systems may reside on different computer based platforms at different locations and run different software. Voting system software is considered to be all executable code and associated configuration files critical for the proper operation of the voting system regardless of the location of installation and functionality provided. This includes third party software such as operating systems, drivers, etc.

6.0.4.1 Software Distribution Methodology Requirements

6.0.4.1.1 Vendors shall document all software including voting system software and third party software (such as operating systems, drivers, etc.) to be installed on voting equipment of the qualified voting system and installation programs.

6.0.4.1.1.1 The documentation shall include a unique identifier (such as a serial number) for the documentation, software vendor name, product name, version, qualification number of the voting system, file names and paths or other location information (such as storage addresses) of the software.

Responsible Entity: voting system vendor
Process: Pre-Voting

6.0.4.1.1.2 The documentation shall designate all software files as static, semi-static, or dynamic.

Responsible Entity: voting system vendor
Process: Pre-voting

Discussion: Static voting system software such as executable code does not change based on the election being conducted or the voting equipment upon which it is installed. Semi-static voting system software contains configuration information for the voting system based on the voting equipment that it is installed and the election being conducted. Semi-static software is only modified during the installation of (a) the voting system software on voting equipment and (b) the election specific software such as ballot formats. Dynamic voting system software changes over time once installed on voting equipment. However, the specific time or value of the change in the dynamic software is usually unknown a priori making it impossible to create reference information to verify the software.

6.0.4.1.2 EAC-accredited testing authorities shall witness the final build of the executable version of the qualified voting system software performed by the vendor.

6.0.4.1.2.1 EAC-accredited testing authorities shall create a complete record of the build that includes: a unique identifier (such as a serial number) for the complete record, list of unique identifiers of write once media associated with the record, time, date, location, name and signatures of all people present, source code and resulting executable file names, version of voting system software, qualification number of the voting system, the name and versions of all (including third party) libraries, the name, version, and configuration files of the development environment used for the build.

Responsible Entity: testing authorities
Process: pre-voting

6.0.4.1.2.2 The record of the source code and executable files shall be made on write once media. Each piece of write once media shall have a unique identifier.

Responsible Entity: testing authorities
Process: pre-voting

Discussion: Write once media includes technology such as a CD-R, ROM, or PROM (but not EEPROM or CD-RW). The unique identifiers appear on indelibly printed labels and in a digitally signed file of the write once media.

6.0.4.1.2.3 The testing authorities shall retain this record until the voting system ceases to be qualified.

Responsible Entity: testing authorities
Process: pre-voting

6.0.4.1.2.4 EAC-accredited testing authorities shall create a subset of the complete record of the build that includes a unique identifier (such as a serial number) of the subset, the unique identifier of the complete record, list of unique identifiers of write once media associated with the subset, vendor, product name, version of voting system software, qualification number of the voting system, all the files that resulted from the build and binary images of all installation programs.

6.0.4.1.2.5 The record of the software shall be made on write once media. Each piece of write once media shall have a unique identifier.

Responsible Entity: testing authorities
Process: pre-voting

6.0.4.1.2.6 The testing authorities shall retain a copy, send a copy to the vendor, and send a copy to the NIST National Software Reference Library (NSRL) and to any other repository named by the Election Assistance Commission.

Responsible Entity: testing authorities
Process: pre-voting

Discussion: The NSRL was established to meet the needs of the law enforcement community for court admissible digital evidence by providing an authoritative source of commercial software reference information. Information is available at www.nsrl.nist.gov.

6.0.4.1.2.7 The testing authorities shall retain this record until the voting system ceases to be qualified.

Responsible Entity: testing authorities
Process: pre-voting

6.0.4.1.3 The vendor shall provide the NSRL or other repository with a copy of all third party software.

Responsible Entity: voting system vendor
Process: pre-voting

6.0.4.1.4 All voting system software, installation programs, third party software (such as operating systems, drivers, etc.) used to install or to

be installed on voting system equipment shall be distributed on a write once media.

6.0.4.1.4.1 All software used to install voting systems shall be received from the voting system vendor, an EAC-accredited test authority, or voting officials.

Responsible Entity: voting officials
Process: pre-voting

6.0.4.1.4.2 Vendors shall document the process used to verify the software distributed on write once media is the qualified software using the reference information provided by the NSRL or other EAC-accredited repository.

Responsible Entity: voting system vendor.
Process: pre-voting

6.0.4.1.4.3 When election officials receive software on write once media, they shall verify that the software is the qualified software by comparing it to reference information produced by the NSRL or other EAC-accredited repository.

Responsible Entity: voting official
Process: pre-voting

6.0.4.1.4.4 The voting system equipment shall verify that the software is the qualified software by comparing it to reference information produced by the NSRL or other EAC-accredited repository before installing the software.

6.0.4.1.4.5 Vendors and testing authorities shall document to whom they provide voting system software write once media.

Responsible Entity: voting system vendor, testing authorities
Process: pre-voting

6.0.4.2 Generation and Distribution Requirements for Reference Information

6.0.4.2.1 The NSRL or other EAC-named repositories shall generate reference information using the binary images of the qualified voting

system software from testing authorities and election specific software from jurisdictions from the write once media.

6.0.4.2.1.1 The NSRL or other EAC-named repository shall generate reference information in at least one of the following forms: (a) complete binary images, (b) cryptographic hash values, or (c) digital signatures of the software.

Responsible Entity: repository
Process: pre-voting

Discussion: Although binary images, cryptographic hashes, and digital signatures can detect a modification or alternation in the software, they cannot determine if the change to the software was accidental or intentional.

6.0.4.2.1.1.1 The NSRL or other EAC-named repositories shall create a record of the creation of reference information that includes: a unique identifier (such as a serial number) for the record, file names of software and associated unique identifier(s) of the write once media from which reference information is generated, time, date, name of people who generated reference information, the type of reference information created, qualification number of voting system (if issued), voting system software version, product name, and vendor.

Responsible Entity: repository
Process: pre-voting

6.0.4.2.1.1.2 The NSRL or other EAC-named repository shall retain the write once media used to generate the reference information until the voting system ceases to be qualified.

Responsible Entity: repository
Process: pre-voting

6.0.4.2.1.1.3 The NSRL or other EAC-named repository that generate hash value and/or digital signature reference information shall use FIPS approved algorithms for hashing and signing.

Responsible Entity: repository
Process: pre-voting

6.0.4.2.1.1.4 The NSRL or other EAC-named repository that generate hash values, digital signatures reference information, or cryptographic keys shall use a FIPS 140-2 level 1 or higher validated cryptographic module.

Responsible Entity: repository
Process: pre-voting

Discussion: See http://www.csrc.nist.gov/cryptval/ for information on FIPS 140-2.

6.0.4.2.1.1.5 The NSRL or other EAC-named repository that generate sets of hash values and digital signatures for reference information shall include a hash value or digital signature covering the set of reference information.

Responsible Entity: repository
Process: pre-voting

6.0.4.2.1.1.6 If the NSRL or other EAC-named repository uses public key technology, they the following requirements shall be met:

6.0.4.2.1.1.6.1 *Public and private key pairs used by the NSRL or other EAC-named repository to generate digital signatures shall be 2048-bits or greater in length.*

Responsible Entity: repository
Process: pre-voting

6.0.4.2.1.1.6.2 *The repository's private keys used to generate digital signature reference information shall be used for no more than three years.*

Responsible Entity: repository
Process: pre-voting

6.0.4.2.1.1.7 Public keys used to verify digital signature reference information shall be placed on a write once media if not contained in a signed non-proprietary format for distribution.

Responsible Entity: repository
Process: pre-voting

Discussion: Examples of non-proprietary standard formats include X.509 or PKCS#7.

6.0.4.2.1.1.8 All copies of public key write once media made by the Repository shall be labeled so that they are uniquely identifiable including at a minimum: a unique identifier (such as a serial number) for the write once media, time, date, location, name(s) of the repository owning the associated private keys, documentation about its creation, and an indication that the contents are public keys.

Responsible Entity: repository
Process: pre-voting

6.0.4.2.1.1.9 The NSRL or other EAC-named repository shall document to whom they provide write once media containing their public keys used to verify digital signature reference information including at a minimum: the uniquely identified public keys, time and date provided, name and contact information (phone, address, email address, etc.) of the recipient.

Responsible Entity: repository
Process: pre-voting

6.0.4.2.1.1.10 When a private key used to generate digital signature reference information becomes compromised, the NSRL or EAC-named repository shall provide notification to recipients of the associated public key that the private key has been compromised and the date of compromise.

Responsible Entity: repository
Process: pre-voting

6.0.4.2.2 The NSRL or other EAC-named repository shall make reference information available on write once media and its associated documentation that is labeled by the repository that created it so that it is uniquely identifiable including at a minimum: a unique identifier (such as a serial number) for the write once media, time, date, location, name of the creating repository, and an indication that the contents are reference information.

Responsible Entity: repository
Process: pre-voting

6.0.4.2.2.1 All write once Reference Information media that do not have a digital signature covering its contents shall be stored in a secure container (such as a safe) when not being used.

Responsible Entity: voting officials
Process: pre-voting

6.0.4.3 Setup Validation Methodology Requirements

6.0.4.3.1 Setup validation methods shall verify that no unauthorized software is present on the voting equipment.

6.0.4.3.1.1 Vendors shall have a process to verify that the correct software is loaded, that there is no unauthorized software, and that static and semi-static voting system software on voting equipment has not been modified using the reference information from the NSRL or other EAC-named repository.

Responsible Entity: voting system vendor
Process: pre-voting

6.0.4.3.1.1.1 The process used to verify software shall not require the execution of software installed on the voting system being inspected.

Responsible Entity: voting system vendor
Process: pre-voting

6.0.4.3.1.1.2 Vendors shall document the process used to verify software on voting equipment.

Responsible Entity: voting system vendor
Process: pre-voting

6.0.4.3.1.1.3 The process shall not modify the voting system software on the voting system during the verification process.

Responsible Entity: Vendor
Process: pre-voting

6.0.4.3.1.2 Vendors shall provide a method to comprehensively list all software files that are installed on voting systems.

Responsible Entity: Vendor
Process: pre-voting

6.0.4.3.1.2.1 The verification process shall be able to be performed using COTS software and hardware available from sources other than the voting system vendor.

Responsible Entity: Vendor
Process: pre-voting

6.0.4.3.1.2.2 If the process uses hashes or digital signatures, then the verification software shall use a FIPS 140-2 level 1 or higher validated cryptographic module.

Responsible Entity: voting system vendor
Process: pre-voting

6.0.4.3.1.2.3 The verification process shall either (1) use reference information on "write once" media received from the Repository or (2) verify the digital signature of the reference information on any other media.

Responsible Entity: voting system vendor
Process: pre-voting

6.0.4.3.1.2.4 Voting system equipment shall provide a read-only external interface to access the software on the system.

- The external interface shall be protected using tamper evident techniques.
- The external interface shall have a physical indicator showing when the interface is enabled and disabled.
- The external interface shall be disabled during voting.
- The external interface should provide a direct read-only access to the location of the voting system software without the use of installed software.

Responsible Entity: voting system vendor
Process: pre-voting

6.0.4.3.2 Setup validation methods shall verify that registers and variables of the voting system equipment contain the proper static and initial values.

Responsible Entity: voting system vendor
Process: pre-voting

6.0.4.3.2.1 The vendors shall provide a method to query the voting systems to determine the values of all static and dynamic registers and variables including the values jurisdictions are required to modify to conduct a specific election.

Responsible Entity: voting system vendor
Process: pre-voting

6.0.4.3.2.2 The vendors shall document the initial starting values of all dynamic registers and variables listed for voting system software except for the values set to conduct a specific election.

Responsible Entity: voting system vendor
Process: pre-voting

6.0.4.3.2.3 Prior to an election voting officials shall query the voting system to determine the values for all the static registers and variables; shall compare these to the vendor documented initial starting values and shall document their findings.

Responsible Entity: voting officials
Process: pre-voting

6.0.4.3.2.4 Any anomalies shall be analyzed and resolved before the election.

Responsible Entity: voting officials
Process: pre-voting

6.0.4.3.3 Voting officials shall run the verification process before each election.

6.0.4.3.3.1 Voting officials shall document the results of the software verification performed on the voting system including at a minimum: a unique identifier (such as a serial number) for the documentation, the date, time, results, location of verification, time, the list of software verified, name of the people that preformed the verification, verification technique used, source of reference information, identifying information of media with reference information (if appropriate), and unique identifiers of the voting systems inspected.

Responsible Entity: voting officials
Process: pre-voting

6.0.4.3.3.2 Any anomalies shall be analyzed and resolved before the election.

Responsible Entity: voting officials
Process: pre-voting